The Post-Pandemic Evolution of Student Data Privacy

Originally published as: Neale, Merritt, and Matt Tryniecki.
“The Post-Pandemic Evolution of Student Data Privacy.”EDUCAUSE Review 55, no. 3, 2020.

As higher education moves to increased remote delivery with the onset of the COVID-19 pandemic, the critical importance of maintaining strong data privacy and governance policies and protocols has only increased.

Data is the lifeblood of any higher education institution’s strategic planning activities, providing both evidence of success and justification for new initiatives. In response to the COVID-19 pandemic, colleges and universities are leaning heavily on new tools and remote methods for collecting various data points about their stakeholders. This wealth of data is a double-edged sword: On the one side are the data applications that improve the student experience; on the other side is the potential for unethical, ill-advised or even unlawful use of personally identifiable information (PII).

In a 2020 EDUCAUSE study (published before the COVID-19 outbreak), higher education leaders identified privacy as their second-mostcritical information technology (IT) issue, with related concerns around information security strategy and digital integrations coming in at No. 1 and No. 4, respectively.[1] As higher education moved to fully remote delivery with the onset of the pandemic, and as delivery for the fall 2020 semester is projected to be fully or partially remote for many institutions, the critical importance of maintaining strong data privacy and governance policies and protocols has only increased. Even when in-person instruction and activities resume, online delivery and the associated new tools and data sets will remain important.

Post-Pandemic Privacy Legislation

To create formal privacy guidelines for educational institutions, the U.S. federal government passed the

[1] Grajek, Susan, and the 2019-2020 EDUCAUSE IT Issues Panel. “Top 10 IT Issues, 2020: The Drive to Digital Transformation Begins.” EDUCAUSE Review Special Report, Jan. 27, 2020. https://er.educause.edu/articles/2020/1/top-10-it-issues 2020-the-drive-to-digital-transformation-begins.

[2] “State Student Privacy Laws.” Student Privacy Compass, Sept. 6, 2020. http://studentprivacycompass.org/state-laws/.

Family Educational Rights and Privacy Act (FERPA) in 1974. But in today's climate, most experts agree that it is outdated and must be revamped to align with a constantly evolving industry.

Since 2013, 41 states have enacted more than 120 supplemental laws.[2] But even these legislative advancements struggle to keep pace with the current rate of technological innovation, driven by rising adoption rates of artificial intelligence and data analytics tools that often render potentially successful information privacy strategies null and void before they can ever be executed.

In the wake of the European Union's rollout of the General Data Protection Regulation (GDPR) in 2018, speculation emerged over whether the United States would implement similar guidelines. Then, in March 2020, new legislation titled the "Consumer Data Privacy and Security Act of 2020" was introduced by the U.S. Senate. Similar to the GDPR and to the California Consumer Privacy Act (CCPA), this legislation calls for establishing the role of a privacy officer, requires comprehensive data security programs, mandates notice and consent, and includes financial penalties for noncompliance. If passed, it would be administered by the Federal Trade Commission(FTC) and would also preempt state law.

Beyond a federal privacy law, colleges and universities may also be required to comply with other statutes post-pandemic. Special Publication (SP) 800-171, issued by the U.S. National Institute of Standards and Technology (NIST), offers security controls for research agencies to protect "Controlled Unclassified Information (CUI) in nonfederal systems and organizations."[3] While this currently applies only to U.S. Department of Defense contracts, the U.S. Department of Education has strongly encouraged institutions to follow the publication's guidelines in their handling of student information, leading many experts to predict that the rule will soon be expanded to include nonresearch data.

In a post-pandemic higher education environment, sustainability will depend on leaders' ability to stay abreast of — and respond appropriately to — the latest changes to state and federal legislation on data security. For example, according to interpretations of the recent guidelines around COVID-19 communications released by the U.S. Department of Education, written permission from students or guardians must be obtained before institutions are legally able to share PII. At the same time, during an emergency, FERPA allows institutions to disclose relevant information about individual students (without prior written consent) to "appropriate parties" (i.e., health departments but not the news media) to protect the health and safety of the community. [4] Colleges and universities should strive to maintain student anonymity whenever possible, highlighting only the information necessary to inform students, staff, faculty and other stakeholders of an imminent threat to public safety.

Looking forward, leaders should also consider how best to translate these and future updates to their institutional policies and how best to communicate these amendments to current and future students.

Ed Tech and Big Tech

Over the last decade, the trend toward technology-enabled "smart" campuses has brought with it heightened scrutiny around the appropriate use of student data. Myriad technologies, including students' smart phones, can be used to track

[3] Ross, Ron, et al. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." NIST, Dec. 2016 (updated June 7, 2018). https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

[4] "FERPA & Coronavirus Disease 2019 (COVID-19), FAQs." Student Privacy Policy Office, U.S. Department of Education. March 2020. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf.

[5] Harwell, Drew. "Colleges Are Turning Students' Phones Into Surveillance Machines, Tracking the Locations of Hundreds of Thousands." The Washington Post, Dec. 24, 2019. https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/.

[6] Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." The New York Times, April 4, 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

everything — from their class attendance and academic performance to their mental and physical health.[5]

The increasingly common partnerships between higher education, third-party vendors and big technology brands (e.g., Amazon, Facebook, Google) further complicate the matter. The involvement of these companies exposes institutions to public scrutiny, fueled by several recent, high-profile violations as well as ambiguity in terms of who is responsible for what might happen to harvested data. [6]

Shadow IT, smart campuses, the Internet of Things and further proliferation of thirdparty systems pose new questions at the intersection of privacy, civil liberties, ethics, ownership and autonomy. Take, for example, the public outcry over Facebook's sale of data to Cambridge Analytica, a political consulting firm that allegedly used the information to target U.S. voters in the 2016 presidential election.[7] The blowback from this scandal has caused leaders in nearly every industry to pause and consider the ethical implications of data collection and its potential uses.

Virtual privacy concerns are not new in higher education, of course. Over the past decade, as most institutions have shifted their delivery models to enable at least some forms of remote learning, corresponding privacy challenges have been uncovered. Yet due to the COVID-19 pandemic, most institutions have had to quickly shift to a completely remote delivery model, which has exacerbated these issues, leaving technology and privacy leaders without the time, support or resources to complete their due diligence with respect to third-party vendors. In addition, the U.S. government is considering using technology platforms (e.g., Google, Facebook, mobile devices) to track the health status of its citizens during the pandemic, and continued remote learning is necessitating an increased use of online vendors (e.g., Zoom, online proctoring companies) — nuances that have the potential to expose colleges and universities to intense public scrutiny about how the data collected from virtual interactions will be used.[8]

Leaders in higher education should be mindful of how these types of third-party platforms are leveraged and should take the initiative to educate students, faculty and staff on what is being collected and how it may be utilized.

Gray Data

Although there is an abundance of ethically neutral or potentially positive uses of students' personal information, there are at least as many questionable, or "gray," areas not covered by current legislation. In these instances, higher education leaders are forced to make difficult decisions.

In an article in the Berkeley Technology Law Journal, Christine L. Borgman, an information studies professor at the University of California, Los Angeles (UCLA), described "gray data" as the data that is collected by colleges and universities about members of their community as part of their daily operations but that falls outside the realm of research. Some data may still be formally regulated or governed, but the challenge is that it often is not.[9]

For instance, consider the myriad data collection points encountered by college or university students on an average day. Getting home late from a night out, a student may use a campus ID card to enter her dorm. The next morning, feeling pangs of hunger, she uses her dining-plan card to pay for breakfast at

[7] Lapowsky, Issie. "How Cambridge Analytica Sparked the Great Privacy Awakening." Wired, March 17, 2019 https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening.

[8] Romm, Tony, Elizabeth Dwoskin, and Craig Timberg. "U.S. Government, Tech Industry Discussing Ways to Use Smartphone Location Data to Combat Coronavirus." The Washington Post, March 17, 2020. https://www.washingtonpost.com/technology/2020/03/17/white-house-location-data-coronavirus/; Harwell, Drew. "Mass School Closures in the Wake of the Coronavirus Are Driving a New Wave of Student Surveillance." The Washington Post, April 1, 2020. https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.

[9] Borgman, Christine L. "Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier." Berkeley Technology Law Journal 33, no. 2, October 2018.

the cafeteria. Later, she reserves a conference room for an organic chemistry study group session that afternoon. After classes are over, she heads to the soccer field, where the performance is tracked by an athlete data management system. And at each stop throughout the day, automated license plate reader (APLR) technology tracks where her vehicle is parked. Multiply these interactions by thousands of students, and one gets a clearer picture of the sheer amount of daily data being collected by higher education institutions.

Given the implications of the COVID-19 pandemic, these ambiguous privacy concerns have been exponentially multiplied as leaders weigh public safety and institutional survival against student privacy and security. Although the data collected can be helpful when developing a student success strategy, it can also be potentially problematic given the implications of tracking individual students' activities across devices, regardless of whether they are on campus or elsewhere.

Gray data challenges can even impact students' post-graduation prospects. Consider the difficult position of an athletic administrator who knows about a promising student-athlete's history of serious head injuries and must determine whether to share this information with professional league recruiters.

The use of gray data, especially data collected virtually, may conflict with campus privacy standards and the concept of reasonable expectations of privacy (which in itself is loosely defined). Yet the current trend toward online delivery and the associated data collection presents a number of potential concerns for both instructors and students. With little to no formal guidance on such scenarios, institutional leaders are often left to determine the ethical path forward on their own.

Building the Infrastructure for Data Governance

To ensure that student data privacy remains an institutional priority during and beyond the current pandemic, higher education leaders should confirm that standards, policies and guidelines are collaboratively developed by a diverse and representative group of stakeholders with broad expertise in student privacy and data protection. This collaboration needs to occur within a welldefined governance structure, with clear roles and responsibilities and defined outcomes.

To that end, over the last few years, colleges and universities have increasingly established the role of chief privacy officer (CPO) and campuswide privacy governance boards. Leadership from these individuals has never been more critical.

Chief Privacy Officers

Previously, CPOs were often relegated to a back-office role on the information security team, but today's effective leaders are becoming visible campus ambassadors, building positive working relationships with diverse stakeholders across all areas of their institutions. During times of crisis like the current pandemic, it is vital to have accessible leaders on the front lines, leading the charge to address urgent needs while strategically positioning the institution for success in an uncertain future.

When a CPO is allowed to have a more visible presence, engaging the campus community and the public at large in a dynamic conversation about privacy, a strong information privacy culture can be built (even in the face of significant challenges). Yet to be truly successful, these administrators need the tools and support to create practical guidelines and policies that can translate into daily practices and procedures relevant in this “new normal.”

Even in the most difficult situations, CPOs should not be the sole arbiters of an institutional privacy policy. They must be willing and able to leverage the knowledge of other internal and external experts to help them make informed and educated decisions. At the same time, they must demonstrate exceptional communication skills and organizational awareness in order to be viewed as a valuable, accessible resource for stakeholders across the institution.

Especially in light of financial constraints brought about by the current recession, institutions may consider enhancing existing IT leaders’ scopes of responsibilities to cover this need for privacy governance (rather than hiring for a new senior-level position). For colleges and universities undergoing a hiring freeze, this presents an opportunity to both grow promising leaders’ skills and leverage existing talent.

Privacy Governance Boards

During a crisis as unprecedented as the COVID-19 pandemic, there are bound to be multiple instances of unusual ethical questions and ambiguous circumstances that will require steadfast leadership, institutional agility and strategic thinking.

With the goal of promoting a balance of perspectives from across the institution, formal privacy governance boards are essential to the ethical review and adjudication of complex information and data management matters. These committees are typically composed of a mix of knowledgeable faculty and administrators, while some integrate students as well. For example, UCLA has its Board on Privacy and Data Protection, whereas the University of Chicago looks to its Data Stewardship Council for guidance. Post-pandemic, these boards will also be essential in creating (or optimizing) and regularly reviewing a crisis response strategy as part of the regular business continuity planning conducted by the institution.

In combination with the privacy office, these boards can help demystify student privacy and data protection concerns inherent in the daily operations of colleges and universities. Further, they can help shape new policies and procedures in response to emerging threats.

The Post-Pandemic Future of Student Privacy

In a post-pandemic future, higher education leaders will continue to grapple with previously unheard-of challenges and gray areas regarding student privacy. In addition, there will likely be a surge in state legislation — with California’s Consumer Privacy Act leading the way — as well as increased rigor around enforcing existing federal laws like FERPA, the Health Insurance Portability and Accountability Act (HIPAA), and Europe's GDPR.

Today, most institutions are just beginning toinvest in the resources required to respond effectively to these developments. Privac offices, while increasingly common in higher education, are still relatively rare. And those that are in place are often understaffed and mired in everyday activities, including breach response, contract reviews and compliance functions.

Likewise, data governance boards are increasing in number, yet many still struggle to make a significant impact on institutional policies. Driving consensus across a wide range of stakeholder groups is a difficult task, often pitting faculty against administration, but leaders have a moral, ethical and professional responsibility to find common ground for the greater good of the institution.

Forward-thinking colleges and universities will embrace this new frontier in higher education by building a robust infrastructure to support ethical data usage, privacy education and innovation. Some actions that leaders can take today to future-proof their institutions against another global emergency include the following:

- Recruiting and/or increasing support for an experienced, qualified chief privacy officer
- Creating or optimizing an institutional data privacy board
- Proactively evaluating third-party vendors as online delivery partners
- Creating and regularly reviewing an institutional crisis response plan
- Assessing institutional data storage and classifications to ensure that privacy protections are optimized
- Communicating with students about updates to privacy policies and simplification of opt-out procedures
- Becoming familiar with existing laws (e.g., HIPAA, FERPA, GDPR, CCPA)
- Calculating potential risks related to dat privacy to help prioritize institutional opportunities for improvement
- Clearly defining ownership for key privacy areas to ensure role clarity and effective execution

As colleges and universities seek to recover from the financial, operational and strategic challenges presented by the COVID-19 pandemic, leaders will be called to juggle numerous highimpact priorities. They may thus be tempted to put privacy matters on the back burner in order to address more urgent demands. Instead, by optimizing infrastructures today, institutional leaders can navigate the operational challenges of COVID-19 and future crises while maintaining a strong commitment to privacy.

HURON

huronconsultinggroup.com